E Safety Policy

Lead : David Price
Reviewed by Governors: Summer 2020
To be reviewed : Summer 2022

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems and school information and data, both in and out of the school.

This Policy has been written to cover all sites belonging to Ysgol Plas Brondyffryn and all users of the School's ICT network and equipment both on the sites and off the premises.. This includes:
Ty'n Fron – Primary Site
Park Street – Secondary Site
Ty'r Ysgol – Secondary Site- SLD
Gerddi Glasfryn – Residential Site
In addition, the policy refers to use of school ICT equipment off-site and the conduct and general working practices specific to ICT of all staff and pupils in any setting - including the home.
Please note that whenever the terms Brondyffryn or School appear they are therefore referring to all of the above sites and settings.

Other School Policies pertinent to this policy include:

- Anti-Bullying Policy
- Child Protection and Safeguarding
- Data Protection Policy
- Freedom of Information Policy
- Information Security Policy
- Records Management Policy
- School Confidentiality Policy
- School Council Policy
- Website Policy

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body /Pastoral Committee on:*	20.06.2016
The implementation of this e-Safety policy will be monitored by the:	School E-Safety Officer E-Safety Committee School Senior Leadership Team Governing Body
Monitoring will take place at regular intervals:	Annually by the e-Safety committee In the review cycle for all policies by the Governing Body
The Pastoral Committee will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	Termly
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	June 2017
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer (Denbighshire and the placing authority if out of county pupil)

	Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - ➢ students / pupils
  - ➢ parents / carers
  - ➢ staff

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals[1] and groups within the school :

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body / Pastoral Committee receiving regular information about e-Safety incidents and monitoring reports.

The Governing body will appoint one member to sit on the e-Safety Committee. This is a Safeguarding role and the governor appointed should be suitably trained/experienced. Their responsibility will include:

- regular meetings with the e-Safety Co-ordinator / Officer
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs (where possible)
- reporting to relevant Governors / sub-committee / meeting

Headteacher / Senior Leadership Team:

- The *Headteacher* has a duty of care for ensuring the safety (including e-Safety) of members of the school community (Day-to-day responsibility for e-Safety is delegated to the School e-Safety Officer)
- The Headteacher and all of the School's identified Child Protection Officers should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the e-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports from the School e-Safety Officer

School e-Safety Officer:

- this role is primarily one of Safeguarding and working with children rather than a technical ICT role
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with the Network Manager
- receives reports of e-Safety incidents and maintains a log of incidents to inform future e-Safety developments.

1

- meets regularly with e-Safety Governor to discuss current issues, review incident logs and if possible, filtering / change control logs
- attends relevant sub-committee of Governors (for the e-Safety report section only if not a Governor themselves)
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The *Network Manager* is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required e-Safety technical requirements as identified by the Local Authority and also the e-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.
- that the filtering policy is applied and updated on a regular basis
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/e-Safety Officer for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- That the School e-Safety Officer is made aware of any new training requirements for users

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (Staff AUP), included as *Appendix 4* in this policy
- they report any suspected misuse or problem to the Headteacher, SLT or School e-Safety Officer for investigation / action
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Safeguarding Officers (Child Protection Officers)

All Child Protection Officers in School/Gerddi Glasfryn will be trained in e-Safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

e-Safety Group

Members of the e-Safety Group will assist the e-Safety Officer with:

- the production / review / monitoring of the school e-Safety policy / documents.
- the production / review / monitoring of the school filtering policy

- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs where possible
- consulting stakeholders – including parents / carers and the students / pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

The e-Safety Group will operate within agreed Terms of Reference included as *Appendix 1* in this document.

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement (Pupil AUP). These are included in the appendices to this document, *Appendix 2* and *Appendix 3*
- need to understand, as far as they are able to, the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- And adherence to the Pupil AUP

Policy Statements

Education – young people

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-Safety curriculum should be provided as part of ICT / PSE / Digital Literacy lessons or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the the Network Manager can temporarily remove those sites from the filtered list for the period of study. The request will be made in writing using the form Request for Special Access to E-Content, included as Appendix 8 in this document. The request will be subject to two criteria: Necessity for learning and e-Safety.

Education – parents / carers

The school will seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day / visiting speakers
- Reference to the relevant web sites / publications

Education & Training – Staff

Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly.
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements.
- The e-Safety Officer will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.
- Child Protection Officers will receive training specific to the responsibilities of this role
- Specific training will be provided for General Data Protection Regulation (EU) 2016/679. The school management will ensure full compliance with DCC/LEA mandatory training requirements in relation to GDPR.

Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-Safety / health and safety / safeguarding . This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents
- Specific training will be provided for General Data Protection Regulation (EU) 2016/679. The Headteacher will ensure full compliance with DCC/LEA mandatory training requirements for governors in relation to GDPR.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS3 and above) will be provided with a username and secure password by The Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (school safe)
- Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the LA by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school manages its own filtering system for any device that doesn’t connect to the LA broadband provision, Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes, all changes go via site Assistant Headteacher who will then pass on to the Network Manager

- The school has differentiated user-level filtering allowing different filtering levels for different ages / stages and different groups of users – staff / pupils.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / are allowed on school devices that may be used out of school.
- Staff are forbidden staff from downloading executable files and installing programs on school devices. Exemptions will be considered depending on need,
- USB memory sticks and similar remote drives are blocked from the school network and users must not attempt to bypass this security measure.
- Use of printers is monitored on a user level, staff and pupils should not use the school printers for any use other than school related use.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Parents / Carers should not share images of pupils in school (e.g sports day) other than their own on social media
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Communications

Staff:
Use of mobile phones/mobile devices: This is strictly limited to staff only areas of the school and either out of work time or during breaks.
Use of School network for non-work related activity is permitted so long as it is in staff only areas of school and takes place out of work time or during breaks. The activity must not be illegal, inappropriate to the workplace or likely to bring the good name of school into disrepute and must not disrupt the normal running of the school network e.g. heavy bandwidth demand.
Communication regarding any and all school matters must be through School systems only (no personal email)
School emails should not be used for non-work related communication.
No photographs/videos should be taken on personal equipment.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- All users' emails are backed up and securely stored in a virtual vault. They will be retained by the school as a permanent record and can be accessed and used in relation to School/LA/County matters or in response to a Freedom of Information Request without the permission of the individual user.
- Users must immediately report to the SLT or E-Safety Officer - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff / staff and students / pupils or parents / carers must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW). Most non-teaching staff are required to register with the Education Workforce Council Wales and are subject to the professional standards of this body. All adults working in the School must understand that the nature and responsibilities of their work places them in a position of trust and that their conduct should reflect this.

The School has a duty of care to provide a safe learning environment for pupils and staff. The School and Local Authority could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School or Local Authority liable to the injured party. All staff working at the School are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the SLT and e-Safety committee to ensure compliance with the School's policies in this area. Inappropriate conduct may expose staff to risk of disciplinary action.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational) – against 'live' opponent			X			
On-line gaming (non educational) - against 'live' opponent					X	
On-line gambling					X	
On-line shopping / commerce			X	S		
File sharing			X	6, S		
Use of social media			X	6, S		
Use of messaging apps			X	6, S		
Use of video broadcasting eg Youtube				S		

S – Staff, 6 – 6th Form

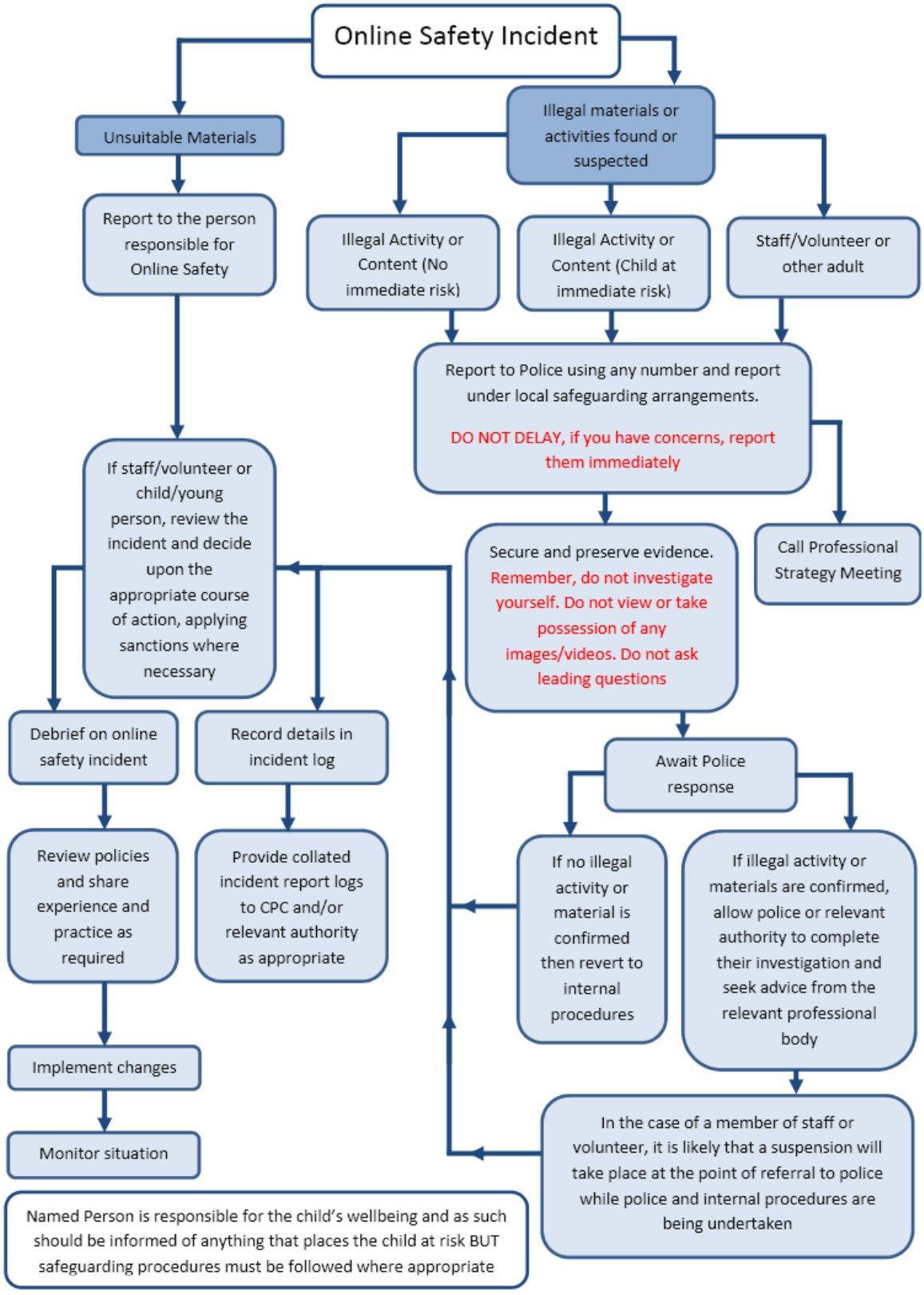
Responding to incidents of misuse

The following procedure will be followed in reporting and investigating incidents of E-Safety concerns where there is a possibility of illegal activity of any description.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the flowchart below for responding to online safety incidents and report immediately to the police.

Procedure in the event of possible illegal activity


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- More than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - ➢ incidents of 'grooming' behaviour
    - ➢ the sending of obscene materials to a child
    - ➢ adult material which potentially breaches the Obscene Publications Act
    - ➢ criminally racist material
    - ➢ other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows (See table below):

Students / Pupils — Actions									
Incidents:	E-Safety Incident Report Completed (first incident)	Refer to class teacher / tutor	Refer to ~~Headteacher~~ / ~~Asst~~ Head	Refer to Police	Refer to technical support staff for action re filtering / security ~~etc~~	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction ~~eg~~ detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X		X	X		X	X		
Unauthorised use of non-educational sites during lessons		X						X	
Unauthorised use of mobile phone / digital camera / other mobile device		X						X	
Unauthorised use of social media / messaging apps / personal email		X						X	
Unauthorised downloading or uploading of files		X						X	
Allowing others to access school network by sharing username and passwords		X						X	
Attempting to access or accessing the school network, using another student's / pupil's account		X			X			X	
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X	X	X		X
Corrupting or destroying the data of other users	X		X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X			X	X		X
Continued infringements of the above, following previous warnings or sanctions	X		X		X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X		X	X		X	X
Using proxy sites or other means to subvert the school's 's filtering system	X		X		X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X		X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X		X	X		X	

All of the above are 'minimum response' to a 'first offence' as far as this can be identified – further action may be taken. Repeated infringement of the code of conduct would require escalation e.g.by reporting to Head Teacher or beginning the disciplinary process.

Staff Actions

Incidents:	E-Safety Incident Report Completed (first incident)	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X		X	X	X				X
Inappropriate personal use of the internet / social media / personal email	X	X	X						
Unauthorised downloading or uploading of files	X	X							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X							
Careless use of personal data eg holding or transferring data in an insecure manner	X		X						
Deliberate actions to breach data protection or network security rules	X		X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X	X					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X		X						
Actions which could compromise the staff member's professional standing	X		X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X						
Using proxy sites or other means to subvert the school's filtering system	X	X				X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X		X						X
Breaching copyright or licensing regulations		X							
Continued infringements of the above, following previous warnings or sanctions	X		X				X		

All of the above are 'minimum response' to a 'first offence' as far as this can be identified – further action may be taken. Repeated infringement of the code of conduct would require escalation e.g.by reporting to Head Teacher or beginning the disciplinary process. Referral to Head Teacher can be facilitated by line manager forwarding a copy of the e-safety report.

Reporting E-Safety Concerns

All E-Safety incidents or concerns about incidents will be reported on the form Reporting E-Safety Incidents, included as Appendix 7 in this document.

School Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *infrastructure / network* is as safe and secure as is reasonably possible and that:

- All collection, use, storage, distribution and disposal of digital information and data is fully compliant with the General Data Protection Regualtion (EU) 2016/679
- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security is the responsibility of The Network Manager

Technical Security

Policy statements

The school will be responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the e-Safety Committee.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place for all mobile devices
- The school reserves the right to remotely control and wipe any device deemed to be a risk to network security, the school may also view the GPS location of a mobile device taken off site.

- School technical staff and teachers regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. Teachers can restrict internet access / control machines used by pupils during lessons as deemed necessary. School uses various methods including the use of LanSchool.
- Remote management tools are used by staff to control pupil workstations and view pupils activity
- Users to report any actual / potential technical incident to the e-Safety Coordinator / Network Manager
- Supply staff will be provided with a supply network login, long term supply staff will be given a login/email upon request of the assistant headteacher. (eg trainee teachers, supply teachers) Site specific supply login cards are held in the office on each site.
- The school provides Guest Wireless access to visitors, the password will be reset every half term. It is the Network Manager's responsibility to ensure that the Guest network is separated from the rest of the school Infrastructure (e.g Servers)
- Staff and students should not download executable files and install programmes on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- When encrypted laptops are taken off site, the responsibility of keeping the password(s) secure is down to the member of staff who has taken the equipment off site.
- Portable devices which are able to be taken off site must be protected by full volume encryption on start-up. Devices which are not protected in this way must not be removed from site.
- Staff who work remotely should ensure no unauthorised use of school equipment or unauthorised access to data while offsite.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Users taking devices off-site must not store password reminders with the devices e.g. in the same bag. In addition the network log-in details of the individual user must not be stored in the same place as the full volume encryption software key - Bitlocker

Policy Statements:

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the e-Safety Committee (or other group).
- All school networks and systems will be protected by secure passwords
- The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (school safe). Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by The network manager. Any changes carried out must be notified to the manager of the password security policy
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Requests for password changes should be authenticated by class teacher/ AHT/ Line Manager to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

Staff passwords:

- All staff users will be provided with a username and password by The Network Manager who will keep an up to date record of users and their usernames.

- The password should be a minimum of 8 characters long and must include one of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- Accounts will be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Student / pupil passwords:

- All users who are able to will be provided with a username and password by The Network Manager who will keep an up to date record of users and their usernames. Usernames / passwords will be given via the Class teacher
- Students / pupils will be taught the importance of password security
- Pupils must never be allowed to use a staff login
- All users - staff and pupils, will log-in with their own username and password. There is no 'group' or 'class' log-in to the school network.

Training / Awareness:

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-Safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review:

The responsible person Network Manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities:

The responsibility for the management of the school's filtering policy will be held by The Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- be logged in change control logs
- be reported to a second responsible person (Site Assistant Headteacher)
- Be authorised by a second responsible person prior to changes being made
- be reported to the e-Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to The Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials. Proxy avoidance sites are strictly forbidden.

Policy Statements:

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

- The school maintains and supports the managed filtering service provided by the Local authority
- The school manages its own filtering service for any device that does not connect to the local authority internet provision (Chromebooks)
- The school has provided enhanced / differentiated user-level filtering through the use of the Sohpos, Securly and OpenDNS filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that use the school internet connection will be subject to the same filtering standards as fixed devices on the school systems
- Laptops taken off site have a built in filter which applies to any internet connection used.
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered initially by the Site Assistant Headteacher who will then liaise with the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the e-Safety Group.

Education / Training / Awareness:

Pupils / students will be made aware of the importance of filtering systems through the e-Safety education programme.. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement.

Changes to the Filtering System:

- All filtering changes should be considered by the Site Assistant Head who will then liaise with the Network Manager
- Block / Unblock requests will be based on the content of the sites and whether it is appropriate for pupils/staff to access. Any illegal / Inappropriate content will not be unblocked.
- The local authority has full autonomy over the categories of blocked sites and has the overriding responsibility, any denied unblocking requests by the Local Authority will not be challenged.
- Logs will be kept of block / unblock requests
- The e-Safety committee + SLT will have access the change control logs

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the site assistant headteacher who will decide whether to make school level changes (as above).

Monitoring:

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School e-Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:*

- *Meraki (Mobile device Management)*
- *LanSchool (View screen/control pupil machines inc Chromebooks)*
- *Sohpos AV (Viewing blocked sites accessed / Warned sites)*
- *Smoothwall Filtering (The LA monitors all websites / blockpages visited)*
- *Securly Filtering (The School solely manages and monitors this filtering system)*

Audit / Reporting:

Logs of filtering change controls and of filtering incidents will be made available to:

- *School SLT*
- *e-Safety Group*
- *e-Safety Governor / Governors committee*
- *Local Authority / Police on request*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Use of Cloud Services

School approved Cloud services:

- Google Apps within the School Education G-Suite (in the YPBD Domain)
- Hwb and all programmes and 'apps' contained within Hwb, including One Drive
- B Squared (Connecting Steps)
- Purple Mash
- Rm EasiMaths
- SumDog

Staff should not use personal accounts for storing school related data on Cloud services.
The Network Manager will maintain an up to date record of approved Cloud services which will be made available to the E-Safety committee.

Log of E-Safety Incident Reports and Actions

All reported E-Safety incidents will be logged. The Log entry will be made by the CPO first contact and will include:

- All the relevant details of the incident
- Actions - these may include longer term actions

- The signature of a second CPO was has consulted on the incident and reviewed the completed log

Training Needs

The training needs of the staff will primarily be identified through the Performance Management Programme (for teachers) and through the Annual Appraisals process (for non-teaching staff). In addition, SLT will identify whole school/specific groups training needs as these arise in response to new initiatives etc.

The School maintains an accurate and up-to-date record of all training activities. This record is reviewed by the Governing Body. Training Specific to E-Safety will be reported to the E-Safety Committee, termly.

Summary of Legislation

The following legislative frameworks may apply to e-Safety matters in the School environment, in relation to adults working with children or in the wider community and have been considered in compiling this policy:

General Data Protection Regulation 2016/679
Computer Misuse Act 1990
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers Act 2000
Trade Marks Act 1994
Copyright, Designs and Patents Act 1988
Criminal Justice & Public Order Act 1994 / Public Order Act 1986
Racial and Religious Hatred Act 2006 / Public Order Act 1986
Protection from Harrassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 and 1964
Human Rights Act 1998
The Education and Inspections Act 2006
The Protection of Freedoms Act 2012

Appendices

Appendix 1: E-Safety Group Terms of Reference

E-Safety Group

Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the [school] community, with responsibility for issues regarding e-Safety and the monitoring the e-Safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The e-Safety committee will seek to include representation from all stakeholders.
The composition of the group should include

- SLT member (If there is no Safeguarding Officers in the SLT)
- School Safeguarding officers
- Teaching staff member
- Non-teaching staff member
- e-Safety School Coordinator (with Safeguarding training and experience)
- e-Safety nominated Governor
- Network Manager
- Student / pupil representation – for advice and feedback. This will be facilitated through the School Council with information/communication in both directions prior to and after meetings of either body.
-

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held termly for a period of 2 hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the e-Safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of e-Safety
- To (at least) annually review and develop the e-Safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-Safety policy
- To monitor the log of reported e-Safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-Safety. This could be carried out through:

    - Staff meetings
    - Student / pupil forums (for advice and feedback)
    - Governors meetings
    - Surveys/questionnaires for students / pupils, parents / carers and staff
    - Parents evenings
    - Website/VLE/Newsletters
    - e-Safety events
    - Internet Safety Day
    - Other methods

- To ensure that monitoring is carried out of Internet sites used across the school (if possible)
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

6. REPORTING

All meetings of the E-Safety Committee will be minuted. These minutes will be provided to and archived by the Governing Body/Sub-Committee as requested by the Governing Body. The e-Safety Governor should be available to the Governing body when the E-Safety report is presented.

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Ysgol Plas Brondyffryn E-Safety Committee have been agreed

Signed by (SLT):

Date: _____

Date for review:_____

Appendix 2: Acceptable Use Policy, Pupil, Basic

E-Safety Policy

Acceptable Use (Pupil, Basic)

This is how we stay safe when we use computers:

I will ask a teacher or another adult from the school if I want to use the computers

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (Pupil):.....

Date:.....

Appendix 3: Acceptable Use Policy, Pupil, Full

E-Safety Policy

Acceptable Use (Pupil, Full)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- If I bring my own portable devices when travelling to school I will hand these in for safe storage during the day.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices

Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems. A copy of the completed form will be sent home to your parents/carers.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, website etc.

Name	
Class	
Signature	
Date	

Appendix 4: Acceptable Use Policy, Staff

E-Safety Policy

Acceptable Use (Staff)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will respond in a timely way to all requests from the Network Manager or SLT to carry out actions with digital devices or the School Network.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

- I will not use personal email addresses to conduct any School activities
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up as advised by the Network Manager
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes on desktop computers, nor will I try to alter computer settings, unless this is allowed in school policies. If I use a School issue tablet device it will be primarily for school use and any programmes and/or digital content I install must not compromise this purpose.
- The School accepts no responsibility for costs incurred by installation of apps on staff School tablet devices.
- Use of School tablet devices should be in accordance with use of School equipment.
- I will surrender any School issued tablet device (or other digital device) on request.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, using encrypted school devices the School's approved cloud storage (Google Apps and Hwb).
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Please Complete and tear off slip below and return to Main Office

---

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Signature	
Date	

Appendix 5: Parental Use Agreement

The School will seek written permission from parents to use video or still images of their children for a range of purposes, as follows:

- For use in essential evidence for learning activities
- For use on displays in School
- For use approved by the School in wider publications including newspapers, film media, the School's own website and Social media

The School will maintain this list and ensure its effective use at all times.

Digital visual images of pupils will be deleted from the School network on a two year cycle, unless expressly retained by staff. Staff will ensure that all images of leavers are deleted from the network at the moment of their leavin

Appendix 6: Guest WiFi User

Guest WiFi – Acceptable Usage Policy

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

1. The use of ICT devices falls under Ysgol Plas Brondyffryn's Acceptable Use Policy, online safety (e-Safety) policy and behaviour which all students/staff/visitors and volunteers must agree to, and comply with.

2. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School owned information systems, including WiFi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.

10. My use of the the Guest WiFi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

12. I understand that my use of the schools internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the schools suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Guest WiFi Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……

Accepted by: ……. Print Name: ……..

This policy will automatically display on any device connected to the Guest Wireless network.

Appendix 7: E-Safety Report Form

Name (Reporting)		Date (Reporting)	
Where did the incident occur		Date of Incident	
Person/s involved in the incident			

Is this a safeguarding concern? If so it must be reported immediately to one of the School Child Protection Officers. Do not wait or just place this report in a pigeon hole!

Briefly described what occurred:
What action has been taken so far?

For the Attention of any School / Gerddi Child Protection Officer

SIgned (Reporting)		Date	
Reported, logged and action by SLT		Date	

Appendix 8: Form, Request Access to Filter Restricted Content

E-Safety Policy

Request Access to Filter Restricted Content

Staff Requesting Access	
For which Class/Pupil/Group	
Date	

Website name / URL	
Type of Content	
Reason access is requested	

Please submit this request to your Assistant Headteacher/Care Manager

SLT Educational/CPO Approved	**SIgn**	**Date**
Network Manager Technical Approval	**SIgn**	**Date**